PACKET-HIDING METHODS FOR PREVENTING SELECTIVE JAMMING ATTACKS

Sayyed Aziz Ahmed Dafedar[1], Sanaulla.S.Kadariinamadar[2], Mohammed Muzamil Mujawar[3]

[1]*M.Tech in Computer Science Engineering, P.A.C.E Mangalore, Karnataka, India*
[2]*M.Tech in Biomedical Electronics & Industrial Instrumentation, P.D.A.C.E Gulbarga, Karnataka, India*
[3]*M.Tech in Computer Science Engineering, K.B.N.C.E Gulbarga, Karnataka, India*

Abstract

In this paper we develop an cryptography where efficient data packet are transferred in an wireless medium. The vulnerability of an wireless medium for its intentional interface attacks for its behaviour as its an open nature leads to intentional interference attacks known as jamming. Making use of these intentional interference attacks we perform lauchpad for mounting the Denial-of-Service attacks on these open wireless networks. As jamming is an external threat model used commonly over an wireless mediums which effects adversely to the protocol specifications which lead to low-effort jamming attacks in an network secreat which is very difficult to mount the error and detect the failure of network. For these problems we address selective jamming attacks in wireless medium network. We create a sensor that has four components. First historic model where detecting known protocol sequence is developed for probabilistic modelSecond is probabilistic model where sizes of packets and inter-packet timing of different packet types are arranged. Third is victim network to produce known sequences for historic analyzer using active jamming mechanism. Lastly online classifier which makes packet type classification decisions For a short period of time and selective targeting messages of high importance are active in these attacks which effect adversely. We evolve an advantage of selective jamming with respect to network adversary efforts and performance degradation is done by case studies such as on routing and attacks on TCP. These selective jamming attacks can be launched by means of performance in real-time packet classification at physical layer of TCP. To overcome these attacks we develop three schemas which prevent real time packet classification by combining cryptographic primitives with physical layer attributesToovercome these attacks we develop three schemas that prevent real-time packet classification by using combined cryptographic primitives with its physical layer attributes.

Keywords: *Jamming attacks, Launch pad, eavesdropping*

----------***----------

1. INTRODUCTION

As wireless networks rely on its uninterrupted availability for interconnecting nodes. However in this medium there are several multiple security threats. Using an transceiver which can lead to eavesdrop in an wireless transmission, another by injecting some messages or jam legitimate ones. Where eavesdropping and unwanted messages can be prevented by making use of crypto systems even then these are very difficult to trace out. As these have been shown for actualize server Denial-of-Service (DoS) attacks against wireless networks. In simple form of jamming adversary interfaces with reception of messages by transmitting jamming signals continuously or by its pulses. As an external threat model jamming strategies include continuous or random transmission of high power interface signals. As jamming is an external threat model. Where it leads to some of the major disadvantages for always sending jamming signals. Some are for expend a significant amount of energy for jamming frequency bands of interest another is continuous presence of unusual high interference levels these attacks makes us easy to detect and trace the error in an medium.

2 EXISTING SYSTEM

Jamming as an external threat model which is considered for jamming attacks on an wireless network medium where jammer is not an part of network medium. Jamming is used for continuous or random transmission of high power interference signals. Anti-jamming rely on spread-spectrum commonly known as SS communications where it provides some protection as per secret pseudo-noise known as PN code here only parties communicating are known. In these it's easy to detect the attacks.

2.1 Disadvantages

1. Jamming attacks are not taken in consideration in internal threat models.
2. Always-on strategy has disadvantages as power consumption and efficiency on an network to jam frequency bands of interest.
3. Cost efficiency is more.

3.SELECTIVE JAMMING IMPACTS

In Selective jamming attacks of a two multi-hop wireless network scenarios. In the first scenario, the attacker targeted a TCP connection established over a multi-hop wireless route. In the second scenario, the jammer targeted network-layer control messages transmitted during the route establishment process.

3.1 Selective Jamming at the Transport Layer

In experiments we adopt a transfer of file between two users for a small file by making use of an multi-hop route. We use TCP protocol for reliable transport of request files between the users. In MAC layer RTS/CTS system mechanisms are enabled. In results we found 11 Mbps speed at each users for an 3 MB of file transmissions on each user links. Placing jammer within proximity of one of the intermediate hops of the TCP connection. In this Four jamming strategies were considered: (a) selective jamming of cumulative TCP-ACKs, (b) selective jamming of RTS/CTS messages, (c) selective jamming of data packets, and (d) random jamming of any packet. In each of the strategies, a fraction p of the targeted packets is jammed.

3.2 Selective Jamming at the Network Layer

In this scenario, we simulated a multi-hop wireless network of 35 nodes, randomly placed within a square area. The AODV routing protocol was used to discover and establish routing paths [19]. Connection requests were initiated between random source/destination pairs. Three jammers were strategically placed to selectively jam non-overlapping areas of the network. Three types of jamming strategies were considered: (a) a continuous jammer, (b) a random jammer blocking only a fraction p of the transmitted packets, and (c) a selective jammer targeting route request (RREQ) packets.

4.MODULES

4.1 Adversary Design

In this module the adversary is in control of the communication medium and can jam messages at any instance of time and any part of the network of its own i.e. it decides by its own for which medium it has to. This adversary module operates in full-duplex mode and thus being able to receive and transmit simultaneously.

4.2 Real Time Packet Classification

In this module real time packet classification at Physical layer is done where packet is encoded, interleaved, and modulated before the transmitting on an wireless channel. At receiver side it is demodulated, de inter leaved and decoded for recovering an original packet by sender side. At sender and receiver we place an jamming node where only few bytes within jammer corrupts by interfering with either user sender or receiver.

4.3 Strong Hiding Commitment Scheme

A strong hiding commitment scheme (SHCS), which is based on symmetric cryptography.

4.4 Cryptographic Puzzle Hiding Scheme

At sender end a packet for transmission. Here the sender selects an random key of a desired length. System generates a puzzle of an key and on time where an puzzle generates a function of an key and on an specified time slot where it has to solve the puzzle with appropriate key in desired time slot.

4.5 Hiding Based on all-or-Nothing Transformations

Transmission of unencrypted packets is pre-processed by AONT it is done before transmission.

4.6 Hiding Based on MD5

Pre-computed MD5 checksum for user files to compare the checksum for an downloaded file. The receiver also performs same packet of sequence while receiving the data packets.

5.ALGORITHM USED

Start Server, Intermediate Server and ‘n’ number of nodes Node chooses a file ‘F’ to send file data to serverIf node chooses the technique ‘SHCS’(A Strong Hiding Commitment Scheme), the message block m is encrypted and encrypted message m| sent to receiver, where receiver decrypts and receives the message block m. If node chooses the technique ‘Cryptographic Puzzle Hiding Scheme (CPHS)’, the message block m is encrypted, a puzzle P and time duration tp is generated at the sender side and sent to receiver, where receive must solve the puzzle in the given duration tp and gets the decrypted message m. If node chooses the technique ‘AONT’ (Hiding Based On All-Or-Nothing Transformations), the message block m is partitioned into n number of blocks. Then the blocks are encrypted and sent to receiver. The receiver the blocks are If node chooses the technique ‘MD5’ (Message Digest), the message block m is split into n number of blocks. Then the blocks are encrypted and sent as four round trips to receiver. In the receiver the blocks are decrypted and the sequence is checked and received.

6.CONCLUSIONS

We consider an internal adversary model in which the jammer is part of the network under attack, thus being aware of the protocol specifications and shared network secrets. Jammer can classify transmitted packets in real time by decoding the first few symbols of an ongoing transmission. The impact of selective jamming attacks is evaluated on network protocols such as TCP and routing. Three schemes have been proposed

that transform a selective jammer to a random one by preventing real-time packet classification. The schemes combine cryptographic primitives such as commitment schemes, cryptographic puzzles, and all-or-nothing transformations (AONTs) with physical layer characteristics.

REFERENCES

[1]. T. X. Brown, J. E. James, and A. Sethi. Jamming and sensing of encrypted wireless ad hoc networks. In Proceedings of MobiHoc, pages 120–130, 2006.
[2]. M. Cagalj, S. Capkun, and J.-P. Hubaux. Wormhole-based antijamming techniques in sensor networks IEEE Transactions on Mobile Computing, 6(1):100–114, 2007.
[3]. A. Chan, X. Liu, G. Noubir, and B. Thapa. Control channel jamming: Resilience and identification of traitors. In Proceedings of ISIT, 2007
[4]. T. Dempsey, G. Sahin, Y. Morton, and C. Hopper. Intelligent sensing and classification in ad hoc networks: a case study. Aerospace and Electronic Systems Magazine, IEEE, 24(8):23–30, August 2009.
[5]. Y. Desmedt. Broadcast anti-jamming systems. Computer Networks, 35(2-3):223–236, February 2001.
[6]. K. Gaj and P. Chodowiec. FPGA and ASIC implementations of AES Cryptographic Engineering, pages 235–294, 2009
[7]. O. Goldreich. Foundations of cryptography: Basic applications. Cambridge University Press, 2004
[8]. B. Greenstein, D. Mccoy, J. Pang, T. Kohno, S. Seshan, and D. Wetherall. Improving wireless privacy with an identifier-free link layer protocolIn Proceedings of MobiSys, 2008
[9]. A. Juels and J. Brainard. Client puzzles: A cryptographic countermeasure against connection depletion attacks. In Proceedings of NDSS, pages 151–165, 1999.
[10]. M. Strasser, C. Popper, and S. Capkun. Efficient uncoordinated fhssanti-jamming communicationIn Proceedings of MobiHoc, pages 207– 218, 2009.
[11]. M. Strasser, C. P¨opper, S. ˇCapkun, and M. Cagalj. Jamming-resistant key establishment using uncoordinated frequency hopping In Pro- ceedings of IEEE Symposium on Security and Privacy, 2008
[12]. B. Thapa, G. Noubir, R. Rajaramanand, and B. Sheng. On the robustness of IEEE802.11 rate adaptation algorithms against smart jamming. In Proceedings of WiSec, 2011
[13]. Uppsala University, The Ad hoc Protocol Evaluation(APE) testbed, release 0.3, downloaded Nov. 2005 http://apetestbed.sourceforge.net

BIOGRAPHIES

Author 1Sayyed Aziz Ahmed Dafedar Presently Perusing MTECH in CSE, P.A.C.E Mangalore.

Author 2 Sanaulla.S.Kadariinamadar Presently Perusing MTECH in Biomedical Electronics & Industrial Instrumentation, PDACE Gulbarga

Author 3Mohammed MuzamilMujawar Presently Perusing MTECH in CSE, Khaja Banda Nawaz College of Engineering Gulbarga.